AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

DETERMINING ELECTRONIC AND CYBER ATTACK RISK LEVEL FOR UNMANNED AIRCRAFT IN A CONTESTED ENVIRONMENT

by

Thomas E. Hay, Capt, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Gregory Intoccia

Maxwell Air Force Base, Alabama

August 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

ABSTRACT

During operations in a contested air environment, adversary electronic warfare (EW) and cyber-attack capability will pose a high level of risk to friendly operational objectives if they are highly dependent on unmanned aerial systems (UAS) mission completion. A UAS EW/Cyber Attack Risk Assessment Matrix is developed using Air Force risk management principles to assess the risk level of three different likely courses of action: low, medium, or high dependence on UAS platforms for overall mission accomplishment. A medium dependence on UAS, considering the strengths, vulnerabilities, and employment of both manned and unmanned platforms, would most often be the preferred way of fully leveraging the abilities of both systems to give the best chance of accomplishing mission objectives. The risk matrix provided in the paper is a tool that can provide commanders insight into the EW/Cyber aspect UAS mission risk, but it should remain open-ended and flexible to allow for continuous assessment of a changing operational environment.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

Unmanned Aerial Systems (UAS), also known as Remotely Piloted Aircraft (RPA) and Unmanned Aerial Vehicles (UAV), have entered into widespread use in the US military since the end of the 20th Century. The number of unmanned aircraft in use by the Department of Defense (DoD) has increased from 50 to over 7,500 in the last 20 years, making up 31 percent of the total inventory of all US military aircraft.[1]

The rise in the demand for unmanned aircraft by U.S. military commanders over this time period is due to both their ability to loiter for long periods of time over a battlefield, as well as the ability to separate their human operators from the dangers of combat operations.[2] Their effectiveness at conducting counterinsurgency operations is facilitated by the luxury of operating in generally permissive airspace, facing little resistance from insurgent forces.

Along with the increase of UAS operations, the Air Force and its Sister Services are refocusing on their ability to operate in contested enemy airspace, otherwise known as an Anti-Access/Area Denial (A2/AD) environment. Senior military leaders have openly stated that over the last 15 years, counterinsurgency (COIN) operations have blunted the Air Force's ability to operate in contested airspace, and that better training and equipment is necessary for mission success.[3]

An A2/AD environment is characterized primarily by a modern Integrated Air Defense System (IADS). Most of the world's nations employ an IADS comprised of advanced Surface to Air Missile (SAM) systems and fighter aircraft, linked together by a survivable, integrated network of surveillance radar systems and Command and Control (C2) centers. The majority of these systems, especially those that may be employed by potential adversary nations to the United States, are developed and manufactured by the Russian and Chinese defense industries.

Designed to defeat supersonic strike aircraft and cruise missiles, a modern IADS would easily overwhelm the majority of the existing Air Force UAS fleet, most of which were designed to loiter in an environment free from an enemy with defensive missile capabilities.[4] A more recent development in Russian- and Chinese-developed air defense networks has been the integration of Electronic Warfare (EW) and Cyber systems designed to generate non-kinetic effects on intruders in partnership with the traditional use of kinetic warheads mounted on missiles. China, in particular, has been developing Integrated Network Electronic Warfare strategies and programs since as early as 1999, with the goal of creating "blindness, deafness or paralysis" via cyber-attacks.[5] These EW and Cyber systems generally focus attacks on the systems which both manned and unmanned aircraft use for awareness, control, and navigation. Particularly for unmanned Air Force aircraft, a goal of aggressor cyber-attacks would be either to separate the aircraft from the control of its human operators, or, in the case of a fully autonomous UAS, to disrupt the electronic information paths the aircraft needs to complete its mission.

The Air Force has published a roadmap for future unmanned aircraft development titled "RPA Vector: Vision and Enabling Concepts 2013–2038," in which it looks to both increase the Service's dependence on current unmanned systems while developing new ones with an ability to operate in and defeat the kinetic, electronic, and cyber threats posed by the next generation of A2/AD airspace.[6] Assuming that recent peer nation investment in cyber and EW capabilities continues at the same pace over the next decade, what level of risk will friendly operations suppose when UAS are employed in contested airspace?

This paper finds that over the course of the next decade of expected developments in the A2/AD environment, adversary electronic warfare and cyber-attacks will pose a high level of risk to friendly UAS operations if operational objectives are highly dependent on UAS mission

completion. Air Force Instruction (AFI) 90-802, *Risk Management*, defines a high risk level to indicate occasional to frequent aircraft loss or loss of mission capability.[7] Unmanned aircraft face this increased risk more often than their manned counterparts due to vulnerabilities in three main areas – the command data link for controlling the aircraft, the data link that provides information from multiple mission sensors to a ground station, and Global Positioning System (GPS) input to the navigation system that enables the aircraft to provide accurate positional data to the operator.[8] Exploitation of all three types of systems has been recently demonstrated by unsophisticated parties, particularly the speculated capture of an RQ-170 by Iran in 2011, while more capable state-level actors have embarked on aggressive programs to boost their own cyber-attack capabilities.[9]

This paper addresses the research question by employing a pragmatic risk management approach and a methodology that documents both quantitative data on system capabilities, along with making qualitative assessments of the use of those systems. Using established Air Force risk management (RM) principles combined with an application of EW/Cyber capabilities help form an open-ended risk analysis matrix that provides the best way to determine a EW/Cyber risk level for UAS operations.

Multiple academic studies – Hartmann, Kim, and Humphreys et al in particular – have identified that the primary EW/Cyber-attack risk to unmanned aircraft lies within the C2 and sensor-data link architecture. Considering this risk component, the Courses of Action (COAs) discussed below are based on the use of various levels of UAS dependence to accomplish operational mission objectives.[10] The risk level of three different likely COAs is investigated: low, medium, or high dependence on UAS platforms for mission accomplishment. In the Recommendations section, information on the measurement of criteria to determine the best

suitable COA for successful mission accomplishment will be analyzed using Air Force RM principles. This is in the form of a UAS EW/Cyber Attack Risk Assessment Matrix that will include definitions for each variable, similar to the Risk Management (RM) matrices currently used by the US military for determining overall levels of operational risk.[11] The cost/benefit tradeoff is explored, and the paper provides recommendations on possible mitigation strategies and technologies, including the tempered use of UAS in unknown and contested environments.

BACKGROUND

All branches of the military are planning to increase reliance on unmanned combat aircraft in the next 25 years.[12] While some senior leaders in the Navy see an almost entirely unmanned strike fighter fleet, the Air Force's vision includes more integration with airborne pilots and operators.[13] Both of these concepts require a complex data link network for C2 and Processing, Exploitation, and Dissemination (PED) of sensor information.[14] While unmanned systems have seen successful use in permissive counterinsurgency operations over the last 15 years, operations over the next decade will require the ability to execute missions in an A2/AD environment. The US Air Force's *RPA Vector: Vision and Enabling Concepts 2013–2038* sees that future unmanned aircraft must be able to "operate effectively in contested or denied" airspace.[15]

To meet this need, operations in A2/AD airspace will require a survivable unmanned aircraft that is capable of protecting itself against traditional kinetic Integrated Air Defense Systems (IADS) as well as from Electronic Warfare (EW) and Cyber-attacks targeted at the sensors, data links, and navigation systems important for mission success.[16] Possible data link vulnerabilities exist in three different architectures: the Ku-band Beyond Line-of-Site (BLOS), C-band Line-of-Sight (LOS) link, and short-range Wi-Fi a/b/g/n wireless local area network (WLAN) connections. The latter two architectures use omnidirectional antennae which increase the chance of interception and jamming. [17] Navigation systems on unmanned aircraft rely heavily on the GPS constellation of satellites. As GPS satellites use similar frequencies to data links, they too are susceptible to jamming and manipulation. Kerns et al have practically demonstrated the ability to completely control an unmanned drone by manipulating the GPS signal it receives with no indication to the operator that the system has been spoofed.[18]

An Air Force Approach to Risk Assessment

In 2012, Air Force Policy Directive (AFPD) 90-8 was released, which mandated the use of Risk Management across every facet of Air Force planning.[19] The directive named the Air Force Safety Center as the primary authority for certifying and controlling RM guidance, which they publish via AFI 90-802, *Risk Management*. The publication describes RM as a tool to help military decision makers choose an appropriate course of action (COA) after weighing the proposed gain of the action versus the risk to the lives and assets of those involved.[20] One of the Air Force's goals for RM include it being involved in all operational mission planning, to "ensure success at minimal cost of resources" and becoming an "inherent part of all military operations."[21]

To help understand the Air Force's approach to RM, four principles are communicated in AFI 90-802, a regulatory publication that both provides an RM framework and directs the use of RM at every level of Air Force planning.[22] First, "no unnecessary risk" will be undertaken. Assuming risk with no chance of a positive mission impact is not recommended. Second, RM decision making will take place "at the appropriate level." Any RM procedure developed should incorporate a clear process for elevating a decision as the risk level increases. Third, at least some form of RM will be incorporated at all levels of planning in the Air Force, regardless of complexity. Though sometimes extensive planning can be impossible in time-constrained environments, risk levels should still be considered in decision making. Fourth, RM must be considered a continuous process. Variables that can either increase or decrease risk levels will change as an operation progresses. It is imperative that Airmen involved in both planning and execution be familiar with specific RM processes so they are able to appropriately adapt to

changing risk variables as they happen. For example, assume an RM assessment for a strike mission grants a medium risk level if a portion of an enemy IADS was inactive. If the mission were only approved for medium risk and the IADS proved to be more active than planned, an Airborne Mission Commander (AMC) would need to fully understand the RM process in order to make an informed decision on whether or not to continue.

The Air Force would describe the example above as "Real-Time RM" as opposed to "Deliberate RM" used during planning.[23] Deliberate RM is described as a process that begins with in-depth study and evolves over an operation's timeline to become a more simplified process. Deliberate RM utilizes the five-step process depicted in Figure 1.

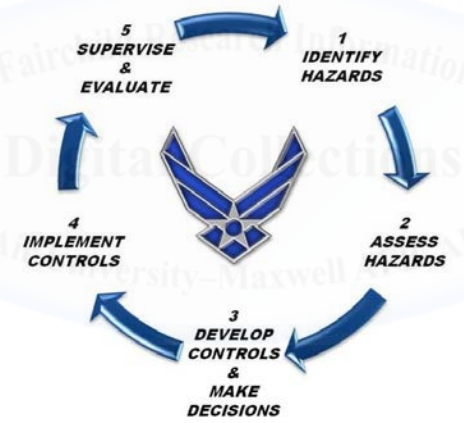

Figure 1. The Five Step RM Process[24]

The first two steps involve identifying and assessing hazards that increase the risk level of a mission. Typically, the most pressing hazards will be those that ultimately result in injury, death, or loss of mission execution capabilities. Hazards are then associated with risk levels should they remain unmitigated. The third step is to develop control measures to mitigate risk and make decisions on what acceptable level of risk (ALR) is appropriate for the mission considering the available controls. The fourth step is the development and application of control

measures that meet the requirements developed in step three. The fifth step is an evaluation of the results and adjustment of the RM process for the next cycle, which will restart at step one and continue until the operation is complete.[25] Figure 2 shows an example Risk Assessment Matrix from AFMAN 90-802, which would be developed from the five-step process above. This paper, using the five-step process, develops a similar matrix for the employment of UAS systems in an environment in which electronic warfare and cyber-attacks are a possibility.

Risk Assessment Matrix				PROBABILITY				
				Frequency of Occurrence Over Time				
				A Frequent (Continuously experienced)	B Likely (Will occur frequently)	C Occasional (Will occur several times)	D Seldom (Unlikely; can be expected to occur)	E Unlikely (Improbable; but possible to occur)
SEVERITY	Effect of Hazard	Catastrophic (Death, Loss of Asset, Mission Capability or Unit Readiness)	I	EH	EH	H	H	M
		Critical (Severe Injury or Damage, Significantly Degraded Mission Capability or Unit Readiness)	II	EH	H	H	M	L
		Moderate (Minor Injury or Damage, Degraded Mission Capability or Unit Readiness)	III	H	M	M	L	L
		Negligible (Minimal Injury or Damage, Little or No Impact to Mission Readiness or Unit Readiness)	IV	M	L	L	L	L
				Risk Assessment Levels				
				EH=Extremely High	H=High	M=Medium	L=Low	

Figure 2. Sample Risk Assessment Matrix[26]

Reference Systems

The following friendly and threat systems are chosen to provide reference information because they represent the types of assets that would be involved in future Air Force A2/AD operations.

RQ-4 Global Hawk

The Northrop-Grumman Global Hawk series is a family of unmanned High Altitude Long-Endurance (HALE) intelligence, surveillance, and reconnaissance (ISR) platforms used by both the US Air Force and Navy. Though the Global Hawk itself is not a combat aircraft intended to employ weapons in a contested environment, the architectures for C2 and data transfer are probably inclusive of what a future Unmanned Combat Aerial Vehicle (UCAV) would use. While all Global Hawks share a similar airframe, their missions and capabilities differ. Most Air Force versions are identified with the RQ-4 designation and can be operationally differentiated by their "Block" numbers. Block 30 aircraft typically employ an electro-optical/infrared (EO/IR) camera and a synthetic aperture radar (SAR), as well as signals intelligence (SIGINT) detection system.[27] Block 40 aircraft carry only a SAR that is optimized as a Ground Moving Target Indicator (GMTI).[28] Additionally, the Air Force has converted some older Block 20 Global Hawks to EQ-4 models; these aircraft act as part of the Battlefield Airborne Communications Nodes (BACN) network to relay radio communications and translate data links over long distances.[29] The Navy uses a Global Hawk variant, currently designated as MQ-4C Triton, to fill a portion of the Broad Area Maritime Surveillance (BAMS) program using an imagery sensor payload roughly equivalent to the Air Force Block 30 variant.[30]

Most Global Hawk variants share commonality in their C2, navigation, and sensor data architecture. All variants use GPS as a primary navigation source, while newer variants source navigation data from a combined GPS/Inertial Navigation System (INS) that is more robust in a GPS-denied environment. For C2 and sensor data communication, during operations outside the range of a ground station, beyond line-of-sight (BLOS) links are used to communicate with a Mission Control Element (MCE) ground station via satellite. Current BLOS data links for C2

include Ultra High Frequency (UHF) SATCOM and the commercial Inmarsat network.[31] Commercial Ku-band (14-15 GHz) satellites are used as the primary means of transmitting sensor data to a ground station.[32] When in range of a ground station, aircraft control and mission data can be passed by a Common Data Link (CDL) line-of-sight (LOS) link. [33]

Global Positioning System

The Global Positioning System (GPS), also known as Navstar, is a type of global navigation satellite system (GNSS) developed and operated by the Air Force. GPS is an evolution of a 1960's satellite system called Transit that was used by US Navy ballistic missile submarines for navigation.[34]

The current GPS system consists of 32 satellites – also known as space vehicles (SVs) – circling the globe twice a day in a Medium Earth Orbit (MEO) of approximately 20,200km altitude.[35] This arrangement ensures that at least four SVs are visible from any point on the Earth's surface.[36] To derive navigation data from these SVs, a GPS receiver will use an internal database and an omnidirectional antenna to measure the extremely small time-of-arrival differences between radio signals emitted by the SVs.[37] Three unencrypted (civilian and military use) and two encrypted (only military use) signals are transmitted over two different L-band frequencies known as L1 at 1575.42 MHz and L2 at 1227.6 MHz.[38] A third civilian signal is currently being broadcasted at 1176.45 MHz, a frequency known as L5, but it is not yet fully approved for navigational use.[39]

GPS-based navigation systems used by unmanned aircraft can be disrupted in two ways – jamming or spoofing. Jamming involves overpowering the GPS L1 and L2 frequencies listed above which renders a navigation receiver unable to acquire GPS signals, whether or not they are

encrypted. Due to the extreme orbital distances and relatively low power of a satellite, jamming is not a particularly difficult task even with commercial off-the-shelf (COTS) equipment. During a test of COTS jammers, a combined University of Texas (UT) Austin and Cornell University team found that a 0.6 watt COTS jammer was able to deny GPS signal acquisition at a distance of 8.7km. Using military hardware to jam GPS signals, as North Korea actively employs during joint US-South Korean military exercises, can render GPS inoperative over a much larger area.[40] The South Korean government, in a public news release, estimates North Korea's GPS jamming equipment – which is partially based on Russian equipment – to be effective at ranges up to 100km from the transmitter.[41]

The second method of GPS disruption is spoofing, which is the ability to "pull" a GPS navigation solution off course by sending slightly more powerful counterfeit GPS signals to a victim receiver. The same group from the Department of Aerospace Engineering at UT Austin cited above were able to reliably demonstrate the ability to spoof unencrypted civilian GPS signals used by a UAS using commercial off-the-shelf (COTS) equipment. During a Department of Homeland Security (DHS) test at White Sands Missile Range in 2012, the team was able to covertly capture a UAS using counterfeit GPS signals without the operator's knowledge, ultimately causing it to crash by sending it erroneous altitude information.[42] Military GPS receivers are generally safe from this type of spoofing, as long as they are using the encrypted signals.[43] If an enemy were to acquire the GPS encryption key via cyber espionage, the system could then be theoretically spoofed. Encrypted military signals are, however, vulnerable to selective-delay attacks as described by Markus G. Kuhn of the University of Cambridge without access to the encryption key. In this type of attack, an encrypted signal could be recorded and retransmitted by a directional high-gain antenna to introduce errors in a GPS receiver's

navigation solution.[44] Additionally, the UT-Austin team notes that both types of spoofing attacks listed above can be enhanced by positional data from a surveillance radar system like those in use by adversarial nations.[45] Kim Hartmann and Christoph Steup posit that the December 2011 capture of an unmanned US RQ-170 by Iranian forces could have been caused by the same GPS spoofing techniques described by the UT-Austin team.[46]

Russian Federation EW Systems

The Russian Federation (RF) defense industry has developed a robust array of EW systems designed to disrupt radar and communications signals, including those which are used for the control and navigation of UAS. Chief of Russian Ground Forces (RGF) Air Defense Troops, Lieutenant General Aleksandr Leonov, states that the Russian military sees EW as the primary means of defeating UAS by attacking their navigation and communications links, and that traditional kinetic air defense systems should only be used to "fill in if needed."[47]

The RGF have entire brigades dedicated to EW, and the centerpiece of those units is the Krasukha-4.[48] The Krasukha-2 and -4 are ground-based, mobile all-terrain, all-weather electronic warfare systems designed by the Russian firm Concern Radio-Electronic Technologies (KRET). Primarily designed to jam airborne surveillance and ground mapping radars, the manufacturer states that the systems can also damage and "suppress radio communication, data transmission systems, and aircraft guidance systems" out to a range of 300km (162nm).[49] Additionally, according to KRET, the "the system can conduct radio interference on a wide frequency range, without restrictions on azimuth or elevation."[50] Whether the system is effective against satellite-based communication is not specified, though KRET has recently stated that a new system is being developed that will "suppress foreign military satellites' radio-electronic

equipment," though the specific capabilities and types of equipment were not named.[51] The Krasukha systems are augmented by KRET's Moskva-1 passive detection systems, which can passively detect and geo-locate complex signal emitters up to a range of 400km (216nm). The Russian Ground Forces have plans to acquire ten Krasukha-4 and ten Moskva-1 systems.[52] The Russian *Telegrafnoye Agentstvo Svazi i Soobshcheniya (*TASS) news agency reported in 2015 that KRET has multiple foreign buyers for the Krasukha-4, though no specific nations or Russian government approval was publicized.[53] In 2007, the DoD stated that China had acquired SATCOM and GPS jammers from Russia that were modified with indigenous Chinese technology.[54]

Russian firm Protek manufactures the R-330ZH Zhitel and P-330MP1 Diabazol truck-based jamming systems that have claimed effectiveness against traditional VHF/UHF radio communications, Inmarsat and Iridium satellite communications, and GPS L1/L2 signals. According to Protek, the system can be set up in under an hour, and can interrupt signals from 100-1900 MHz in a 900 km^2 ($262nm^2$) area for up to 24 hours at a time. The system can additionally collect SIGINT data in the same frequency range.[55]

The RGF have most recently employed their extensive EW systems in the conflict between the Ukraine and pro-Russian rebels.[56] According to US Army Lt Gen Ben Hodges, Russian EW systems deployed to the area successfully shut down all of the Ukrainian military's communication systems. Bret Perry, writing in an article on the DefenseOne website, reports that Russian jamming activity would only cease for short periods in attempts to geo-locate Ukrainian units that were finally able to transmit.[57] During a Special Monitoring Mission (SMM) in the Ukraine, the Organization for Security and Cooperation in Europe (OSCE) experienced such heavy GPS and data link jamming that they were unable to employ their S-100

unmanned helicopters to monitor rebel-held areas.[58] The S-100, built by German firm Schiebel, is capable of using electro-optical, radar, and SIGINT sensors that can transmit real-time data of a C-band (4-8 GHz) link to a ground station up to 200 km (108 nm) away, flying at speeds of 222km/h (120 knots).[59]

Adversary Nation Cyber Warfare

The Joint Chiefs of Staff, in their publication Joint Operating Environment (JOE) 2035, see cyberspace as sovereign territory that must be protected from adversary attacks. Likewise, competitor nations such as China look to use cyberspace to "preserve sovereignty, national security, and societal public interest."[60] The JOE 2035 assessment further states that the competitive environment for military cyber operations will include "any digital, code-enabled system that can communicate, emit, connect, or sense."[61] Attacks against these assets, sometimes resulting in physical damage, can be executed globally with little regard for physical distance between attacker and target.

The Chinese People's Liberation Army (PLA) is actively developing a robust offensive cyber-attack capability with the aim of degrading and destroying an enemy's C2 networks. The PLA calls their combination EW/Cyber strategy Integrated Network Electronic Warfare (INEW). In accordance with the PLA's highest objectives of early information dominance, INEW is a cohesive preemptive strategy designed to be employed early and continuously against C2 and ISR assets.[62] The US-China Economic and Security Review Commission assesses that China is utilizing civilian hackers to amass zero-day exploit (ZDE) tools that can be used to initiate network infiltrations. ZDE tools are generally designed to take advantage of security holes that developers and administrators are unaware of until they are compromised. Once a vulnerability

is discovered, however, security gaps are typically patched, giving ZDE tools a short expiration date.[63]

Assessing the PLA's specific capability to carry out cyber-attacks on C2 systems used by UAS is difficult. RAND, in their US-China Military Scorecard, give the US an overall advantage against Chinese cyber capabilities in a possible conflict, though they caveat their findings with the acknowledgement that unclassified information on the subject is extremely limited.[64] They assess a slight downward trend in the US cyber advantage, which is most heavily dependent on the intelligence ability of the National Security Agency (NSA).

RESEARCH

Methodology

How can Air Force operations planners define the EW/Cyber risk level against UAS as it pertains to mission accomplishment? This paper will propose a pragmatic and open-ended solution in the form of a risk assessment matrix in line with the Air Force approach to RM described in the Background section above. The matrix is designed to be used as both a deliberate planning tool and continuously thereafter as real-time operations progress. As described in the Five Step Air Force RM process, any approach to risk management should be seen as a continuous circle of development and evaluation.

To develop the categories to be measured in the matrix, the background research was used to gain understanding of the nature of various EW/Cyber systems and their probable effects on friendly UAS. The research found that two variables are inherent in any EW/Cyber system's ability to attack a UAS. First, its ability to affect an adversary system must be compared versus the friendly system's ability to resist the attack – this is encapsulated in the capability assessment in the matrix, which is further defined below. Second, the range at which the EW/Cyber system can be employed is also a critical factor – this is categorized as reach in the matrix. How far the enemy system can project the capability effects is just as critical as the effects themselves. In addition to capability and reach, it is important to know the enemy's intent to use any EW/Cyber tools they have. Some military operations may take place during peacetime, where an otherwise capable enemy may decide not to employ their tools. On the other hand, during full-scale hostilities, an unrestrained enemy would be likely to use every EW/Cyber method available to them. To account for the varying level of will to use these tools, the intent category is included.

Measuring Criteria

The values assigned to the categories of capability, reach, and intent, are low (1 point), medium (2 points) and high (3 points). Though numerical values would seem to produce an objective outcome, that is not the intent of the matrix. It should remain a fluid assessment of enemy ability combined with friendly intentions. Risk itself is an abstract concept; attempting to quantify it in order to solely justify a course of action is not recommended.

For Air Force planners to assign values to the matrix categories for real-world operational planning, extensive Intelligence Preparation of the Environment (IPOE) should be conducted that compares the enemy's offensive EW/Cyber capabilities with the friendly UAS vulnerabilities to those attacks. Air Force doctrine defines IPOE as a process to analyze adversary abilities and "the effect of the operating environment on both friendly and enemy COAs." The primary tool to perform IPOE is the global integrated ISR enterprise, which focuses partly on the contrasting abilities of both enemy and friendly EW/Cyber networks and how they affect friendly access to the operating environment.[65] In line with the Real Time RM process, IPOE must shift to a continuous intelligence assessment of the environment once an operation has begun and initial assumptions change. For the outcomes explored below, the precise nature of both offensive and defensive EW/Cyber systems is outside of the scope of this paper. Additionally, considering the pace of advancement in the electronic arena, any benefit gained by conducting detailed system versus system analysis would only be of short-term use.

UAS EW/Cyber Risk Matrix

The following UAS EW/Cyber Risk Matrix is a proposed points-based Deliberate RM tool to be used by planners in operations involving unmanned systems. Though the matrix

produces a numerically quantifiable risk level, the categories themselves contain purposeful ambiguity to leave room for fluid assessment and judgment regarding enemy capabilities and friendly intent. Real-Time RM, in accordance with the AFI 90-802 directives described above, would also be used as assessments are refined or enemy capabilities change. The matrix is divided into three categories of enemy EW/Cyber capacity – capability, reach, and intent. The exact meanings and intent of these categories is contained in the "Threat Matrix Definitions" section below. To use the chart, an assessment of each category would be rated as low, medium, or high and be assigned one, two, or three points, respectively. The total from all three categories will then be affected by the most important factor, the Friendly Dependence on UAS multiplier. A low dependence will have no effect on the RM score, while a medium and high dependence will multiply the score by two or three, respectively. Completing the table will produce an RM score, which calculates an overall risk level of low (<13 points), medium (13-17 points), or high (>17 points). Point values in each category were designed to produce logical risk assessment outcomes. The correlation between the specific point range and risk level was determined by examining all possible combinations of points values and dependence level. The Courses of Action section will use practical and hypothetical examples to illustrate risk outcome possibilities.

	Low (1 Point)	Medium (2 Points)	High (3 Points)
Enemy EW/Cyber Capability			
Enemy EW/Cyber Reach			
Enemy EW/Cyber Intent			
Subtotal			

	Low (No Multiplier)	Medium (x2 Multiplier)	High (x3 Multiplier)
Friendly Dependence on UAS			
Total Risk			

1-12: Low Risk 13-17: Medium Risk >17: High Risk

Table 1. UAS EW/Cyber Risk Assessment Matrix

Risk Matrix Definitions

Enemy EW/Cyber Capability is defined as the threat group's capability to attack UAS C2, navigation, and sensor-data architectures that are expected to be employed in military action. This assessment takes into account an estimate of the friendly force's ability to insulate against such attacks. A "low" capability indicates that the enemy does not possess the ability to conduct EW or cyber-attacks in a capacity that would seriously interfere with UAS operations – if they do possess such tools, they are unreliable or only able to employ them sparingly against an extremely limited number of targets. Additionally, the enemy may be assessed to have expended most or all of its Zero-Day Exploit (ZDE) cyber capabilities. "High" capability in this area indicates that an enemy force has a very robust, well-trained, and militarized EW/Cyber force that can execute multiple sophisticated attacks simultaneously against many targets, and are assessed to still hold ZDE tools in reserve. A "medium" capability is a mixture of "low" and

"high" capabilities that is at the discretion of the assessor. The "medium" category can also account for possible unknowns in an enemy's ability.

Enemy EW/Cyber Reach is a measure of the enemy's ability to project its EW/Cyber capabilities over certain distances. A "low" reach generally indicates an enemy ability to only affect friendly targets that are within line-of-sight of the EW/Cyber source. "medium" reach would generally indicate an enemy ability to project EW/Cyber effects across a theater level – including against space assets that are transiting the theater. The capabilities of the Krasukha-4 described above to jam friendly communications and C2 data links – such as the RQ-4's commercial and military SATCOM links – out to an advertised 162nm distance would probably be assessed with a medium reach, especially when paired with a passive detection system such as the Moskva-1. GPS jamming systems such as the Protek R-330 series would also be considered medium-reach assets if they were assessed to be able to generate effects on a UAS at its normal operating range. A high level of reach would show an enemy ability to conduct targeted attacks over global distances, and would be almost exclusively cyber in nature. In this case, an enemy could target the highest levels of national C2 no matter where they lie around the world. In all cases, reach should not be thought of as a specific measure of distance, but a measure of effectiveness. As an example, if friendly UAS were typically able to employ the required sensors or weapons well outside of the effective range of an enemy EW system, the enemy's reach could be rated as low since it is not a factor to the UAS. Conversely, without any physical change in actual enemy capability or reach, a requirement for a friendly UAS to operate inside this range would effectively increase the reach risk.

Enemy EW/Cyber Intent is a measure of an enemy's willingness to use its capabilities against friendly UAS. Multiple factors would affect this assessment, including the level of

conflict and the enemy's perceived threat level. As EW/Cyber-attack could be considered an act of warfare, the enemy's intent to use the full gamut of capability to disrupt UAS operations during peacetime would likely be low. During periods of elevated tension, an enemy may be assessed to be using only a limited portion of its capabilities, wanting to reserve ZDE and other tools to higher levels of conflict, which could warrant a "medium" intent to use. Friendly ability to counter enemy EW/Cyber systems could also affect an enemy's level of intent. For example, if friendly forces are able to easily find, target, and destroy an enemy jamming system when it is turned on, this could reduce the enemy's intent to use that system in certain scenarios.

Friendly Dependence on UAS is a measure of the burden placed on friendly UAS assets towards accomplishing the desired mission objectives. This category acts as a multiplier for the aggregated total of the prior three risk categories to determine the overall level of EW/Cyber risk versus UAS mission effectiveness. The exact proportion of UAS involvement, measured as a numerical percentage, may not necessarily meet the intent of this category. Rather, "dependence" should be treated more as an intangible measure of the level of responsibility placed on unmanned assets. A "low" level of dependence indicates that the large majority of mission-related flight operations are conducted by manned aircraft. This includes support assets such as ISR, tanker and cargo aircraft, which, while not directly responsible for enemy engagement, are enablers necessary for combat aircraft to successfully complete their mission. A "medium" level of dependence indicates a higher proportion of mission-critical operations are carried out by unmanned aircraft. A greater number of support roles being performed by unmanned aircraft could lead to a medium dependency rating, as long as the loss of mission effectiveness of these roles did not lead directly to overall defeat. A "high" dependency rating would reflect a strategy in which the effectiveness of unmanned systems was critical to overall

mission success. Again, this rating does not necessarily stem from a particular percentage of air operations that are conducted by unmanned aircraft, rather it is an assessment of the unmanned fleet's level of responsibility towards accomplishing the operation's objectives. One indicator of a high dependency would be a large proportion of critical strike or anti-air operations being conducted by unmanned assets. Additionally, if most of the direct combat operations are conducted by manned aircraft, but those aircraft were significantly reliant on ISR, tanker, or other support aircraft that were unmanned, a high dependence level could also be required.

RESULTS

The three courses of action described by this paper refer to the level of dependence – low, medium, or high – of the Air Force on unmanned systems to meet military objectives at any level of operations. The definition of "dependence" is variable, as described in the Risk Matrix Definitions section above. It is important to note that the three COAs do not necessarily refer to the overall force structure of the Air Force, but rather should be viewed as the level to which unmanned assets are required to achieve desired goals or objectives. A particular mission could have different levels of dependence on UAS than a theater-wide operation. It is important to note that with each COA below – and Air Force operations in general – the specific employment of systems used to accomplish certain objectives is critical for real-world application. Though the exact employment and type of systems to be used for a particular scenario is outside the scope of this paper, generalized examples will be given in order to illustrate the main points.

Low Friendly Dependence on UAS

Using the Risk Matrix, a low dependence by friendly forces on UAS equates to a low risk level for EW/Cyber-attack against the unmanned systems to affect mission accomplishment, even if the enemy is given high ratings in capability, reach, or intent.

Using a practical example for illustration, a mission using manned airlift and tanker assets might involve SIGINT support from an unmanned high-altitude RQ-4 Block 30 Global Hawk. Planners might see the RQ-4 as a "nice to have" asset that can enhance safety, but not as a required element for mission accomplishment. If they were to see the unmanned asset as a more significant asset, then the dependence level would be increased accordingly and would fall in a different course of action. In this example, however, they do not, so the overall UAS

EW/Cyber risk level for mission accomplishment is Low. Using results from the chart, a low risk (in all cases, no greater than 9) is derived no matter how much the enemy is able to attack the UAS. Table 2 is a truncated version of the larger risk matrix that specifically shows the results for high enemy EW/Cyber abilities with a low friendly dependence on UAS.

	High (3 Points)	Friendly Dependence on UAS	**Total Risk**
Enemy EW/Cyber Capability	3	Low (No Multiplier)	**9**
Enemy EW/Cyber Reach	3		
Enemy EW/Cyber Intent	3		

1-12: Low Risk 13-17: Medium Risk >17: High Risk

Table 2. Risk Matrix Results for Low Dependence

While a low dependence on UAS in the Risk Matrix will always generate a low EW/Cyber risk level, assuming that low dependence is automatically the most preferable COA ignores the benefits that UAS can bring to military operations. Advantages such as long-endurance paired with relatively low operating costs, as the *USAF RPA Vector* states, are very useful in operations that require a persistent look at enemy high value targets while minimizing the risk to US personnel.[66] Current (2016) US military operations such as INHERENT RESOLVE and FREEDOM'S SENTINEL are counterinsurgency-focused and benefit greatly from UAS like the MQ-1 and MQ-9.

Medium Friendly Dependence on UAS

A medium friendly dependence on UAS for mission accomplishment will generally produce low or medium risk outcomes using the matrix. When the enemy is given high assessments in capability, reach, and intent, the risk level just crosses the high threshold.

An example of an operation with medium dependence on UAS to execute mission-critical tasks would be a major contingency operations (MCO) scenario against a state-level adversary in which UAS serve in support roles such as ISR and communications nodes. For the purposes of this scenario, the manned-unmanned aircraft mix mirrors the current USAF aircraft force structure, minus the MQ-1/9 family of aircraft. Mission-critical assets such as strike and offensive counter-air (OCA) aircraft are almost exclusively controlled by pilots in the cockpit, as are tankers, transports, and battlefield C2 aircraft. UAS assets can fill a variety of roles in this environment in the areas of communications nodes and SIGINT gathering. Aircraft such as the EQ-4 BACN would act as Tactical Data Link (TDL) translators, exploiting their ability to orbit at high altitudes for extended periods of time while translating TDL languages amongst manned assets and C2.[67] Other UAS platforms, including additional versions of the RQ-4 Global Hawk, would be used to gather electronic intelligence (ELINT) on enemy radar and communication systems from a standoff distance generally outside the range of the enemy's defensive missile systems.

If the enemy's capability, reach, and intent were all assessed to be high, a medium friendly dependence on UAS for mission accomplishment would push the EW/Cyber risk to UAS to 18 – just above the high risk threshold. A reduction in any one aspect of enemy ability to a medium level – for example, to account for an unknown quantity as mentioned in the Definitions section above – reduces the overall risk level to the medium range as shown in Table 3 below.

		Friendly Dependence on UAS	Total Risk
Enemy EW/Cyber Capability	3	Medium (x2 Multiplier)	**16**
Enemy EW/Cyber Reach	2		
Enemy EW/Cyber Intent	3		

1-12: Low Risk 13-17: Medium Risk >17: High Risk

Table 3. Risk Matrix Results for Medium Dependence

High Friendly Dependence on UAS

A high dependence on UAS systems for mission accomplishment can generate a variety of outcomes, from low to high risk levels for EW/Cyber effects on friendly UAS, depending on their capability.

This current nature of US conflicts in Iraq and Afghanistan involve enemies with very little ability to harm unmanned aircraft using EW/Cyber tools. To reflect this scenario, low scores are assigned to the enemy capability, reach, and intent categories, with a high friendly dependence multiplier indicating the extensive use of unmanned systems by the US. This produces a 9 (low) overall risk level – friendly forces are essentially able to operate unmanned aircraft in any way they see fit, with little danger of enemy interference in the EW/Cyber spectrum.

Should the enemy in those or similar conflicts acquire a medium level of capability and reach with a corresponding medium level of intent to employ it, the risk increases to 18 – just above the high threshold if friendly forces continue with a high dependence level. These results are shown in Table 4 below. Only by reducing friendly dependence on UAS will the overall risk reduce.

	Medium (2 Points)	Friendly Dependence on UAS	**Total Risk**
Enemy EW/Cyber Capability	2	High (x3 Multiplier)	**18**
Enemy EW/Cyber Reach	2		
Enemy EW/Cyber Intent	2		

1-12: Low Risk 13-17: Medium Risk >17: High Risk

Table 4. Risk Matrix Results for Medium Ability and High Dependence

Another interesting scenario is that of peacetime operations near an adversary nation. State-level actors with high levels of capability and reach, but with a low intent to use also generate a high overall risk to Air Force operations that are highly dependent on UAS platforms. A practical example of this would be current US operations in the South China Sea area.[68] An intelligence assessment of China's EW/Cyber capabilities and reach would likely yield a medium to high rating, but with a low intent to employ them since the US and China are not actually at war. As shown in Table 5, this still yields a medium risk level during operations if the US is highly dependent on UAS for mission accomplishment. The risk would immediately transition to high as should the adversary decide to employ their EW/Cyber capabilities against friendly UAS.

	Medium (2 Points)	Friendly Dependence on UAS	**Total Risk**
Enemy EW/Cyber Capability	2	High (x3 Multiplier)	**15**
Enemy EW/Cyber Reach	2		
Enemy EW/Cyber Intent	1		

1-12: Low Risk 13-17: Medium Risk >17: High Risk

Table 5. Risk Matrix Results for Medium Ability, Low Intent, and High Dependence

RECOMMENDATIONS

From the three COAs explored above, it is clear that the risk level associated with operating UAS against an enemy with EW/Cyber capabilities is strongly associated with the level of dependence that friendly forces place on the UAS to accomplish critical mission objectives. A low dependence level generally produces the lowest level of risk regardless of an enemy's EW/Cyber ability, but since it ignores many of the inherent benefits of UAS operations – particularly the ability of some long-endurance UAS to loiter for extended periods of time near a battlefield – it is not the most preferable COA. A COA with a high dependence on UAS is also not the most preferable – with only a marginal increase in enemy capability or intent to use it, the overall mission is immediately put at a high risk level should the UAS be rendered ineffective.

The most preferable COA that remains is that of medium dependence of UAS systems for mission accomplishment. Based on the examples given above, this assessment is valid for multiple types of operations that the Air Force may be involved in. The most challenging scenario, however, is that of major contingency operations against a peer-level enemy capable of generating an A2/AD with EW/Cyber capabilities against friendly aircraft. In this MCO environment, considering a medium level of friendly dependence on UAS, friendly objectives are enhanced by the employment of UAS, but not wholly dependent on them. UAS with ELINT capabilities can help C2 identify enemy radar systems for destruction, while UAS with BACN equipment will help C2 distribute that information quickly to both strike assets for destruction and all other assets for threat warning. Importantly, to meet the goal of medium dependence, if the UAS assets listed above are rendered ineffective by an enemy's EW/Cyber weapons, the manned aircraft could still accomplish the overall mission objectives, though at a reduced level of effectiveness.

CONCLUSION

Referencing the COA outcomes and recommendations above, it is reasonable that adversary electronic warfare and cyber-attacks will pose a high level of risk to friendly mission accomplishment if operational objectives are highly dependent on UAS mission completion. To maintain a medium EW/Cyber risk level for UAS involvement in Air Force operations, the key term to remember is "desired, not required." Unmanned assets have great abilities in the area of long endurance and relatively low cost; ignoring these benefits by leaving UAS out of a mission package solely to reduce risk would be leaving possible enhancements to nearly any military operation unused.

On the opposite end of the spectrum, relying too heavily on UAS to accomplish a desired mission against an enemy capable of effective EW/Cyber-attacks leads to a high risk level that is generally unacceptable. A medium dependence, considering the strengths, vulnerabilities, and employment of both manned platforms and UAS, would most often be the preferred way of fully leveraging the abilities of a UAS to give the best chance of accomplishing mission objectives.

The UAS EW/Cyber Risk Matrix provided above, or a similar product, is one tool that can provide commanders insight into the EW/Cyber aspect of mission risk regarding UAS. As described above, the matrix is intentionally open for interpretation by intelligence and operations personnel to provide overall assessments of enemy versus friendly systems. This provides flexibility to the risk assessment outcome, while also allowing for continuous assessment of the risk level as real-world operations progress and change.

NOTES

[1] Spencer Ackerman and Noah Shachtman, "Almost 1 In 3 U.S. Warplanes Is a Robot," *Wired Danger Room*, January 9, 2012.
[2] United States Air Force. "RPA Vector: Vision and Enabling Concepts 2013–2038." Headquarters, United States Air Force (17 February 2014): 14.
[3] Amber Corrin. "The Air Force's Anti-Access Area Denial Problem." C4ISR & Networks (16 September 2015). http://www.c4isrnet.com/story/military-tech/isr/2015/09/15/air-force-anti-access-anti-denial/72317652/.
[4] United States Air Force. "RPA Vector:" 11.
[5] Bryan Krekel. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Northrop Grumman Corporation (9 October 2009). http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf: 14-15.
[6] United States Air Force. "RPA Vector:" 32.
[7] Air Force Instruction (AFI) 90-802. *Risk Management*. Air Force Safety Center (23 March 2015). http://static.e-publishing.af.mil/production/1/af_se/publication/afi90-802/afi90-802.pdf
[8] Hartmann, Kim and Steup, Christoph. "The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment." NATO Cooperative Cyber Defense Centre of Excellence Publications, 2013. https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf: 3-4.
[9] Scott Peterson. "Iran Hijacked US Drone, Says Iranian Engineer." Christian Science Monitor (15 December 2011). http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.
[10] Hartmann and Steup: 4.
[11] AFI 90-802: 16.
[12] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. "Unmanned Systems Integrated Roadmap FY2011-2036." Department of Defense (2011): v.
[13] Kris Osborn. "Navy Secretary Says Future Navy Fighter Planes Will Be Unmanned." Military.com (16 April 2015). http://www.military.com/daily-news/2015/04/16/navy-secretary-says-future-navy-fighter-planes-will-be-unmanned.html.
[14] Hartmann and Steup: 4-8.
[15] United States Air Force. "RPA Vector:" 32.
[16] Ibid.
[17] Hartmann and Steup: 10-12.
[18] A.J. Kerns, D.P. Shepard, J.A. Bhatti, and T.E. Humphreys. "Unmanned Aircraft Capture and Control via GPS Spoofing." *Journal of Field Robotics*. 31(4): 617–636, 2014. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf.
[19] Air Force Policy Directive (AFPD) 90-8. *Environment, Safety and Occupational Health Management and Risk Management.* Air Force Safety Center (2 February 2012): 8-9.
[20] AFI 90-802: 3.
[21] AFI 90-802: 4.
[22] AFI 90-802: 12-13.
[23] AFI 90-802: 13-14.
[24] AFI 90-802: 15.
[25] AFPAM 90-803: 18.
[26] AFI 90-802: 16.

[27] Northrop Grumman. “RQ-4 Block 30 Global Hawk Datasheet.” Northrop Grumman Systems Corporation (2012). http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Datasheet_GH_Block_30.pdf.
[28] Northrop Grumman. “RQ-4 Block 40 Global Hawk Datasheet.” Northrop Grumman Systems Corporation (2012). http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Datasheet_GH_Block_40.pdf.
[29] Northrop Grumman. “Battlefield Airborne Communications Node.” http://www.northropgrumman.com/Capabilities/BACN/Pages/default.aspx (Accessed 24 August 2016).
[30] Northrop Grumman. “MQ-4C BAMS UAS Datasheet.” Northrop Grumman Systems Corporation (2011). http://www.northropgrumman.com/Capabilities/BAMSServiceSupportandTraining/Documents/pageDocs/bams.pdf.
[31] Northrop Grumman. “Q-4 Enterprise.” Northrop Grumman Systems Corporation (2012). http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Brochure_Q4_HALE_Enterprise.pdf.
[32] Ibid.
[33] Ibid.
[34] Howell, Elizabeth. “Navstar: GPS Satellite Network.” Space.com (14 February 2013). http://www.space.com/19794-navstar.html.
[35] U.S. Naval Observatory. “Current GPS Constellation.” (Accessed 24 August 2016). http://tycho.usno.navy.mil/gpscurr.html.
[36] National Coordination Office for Space-Based Positioning, Navigation, and Timing. “Space Segment.” (Accessed 24 August 2016). http://www.gps.gov/systems/gps/space/.
[37] Howell.
[38] Department of Defense. “Global Positioning System Standard Positioning Service Performance Standard (4th Edition).” (September 2008). http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf: 4.
[39] Dunn, Michael J. “Navstar GPS Space Segment/User Segment L5 Interfaces.” Global Positioning Systems Directorate (24 September 2013). http://www.gps.gov/technical/icwg/IS-GPS-705D.pdf: 8.
[40] Shim, Elizabeth. “North Korea Sent 2,100 GPS Jamming Signals to South.” United Press International (29 June 2016). http://www.upi.com/Top_News/World-News/2016/06/29/North-Korea-sent-2100-GPS-jamming-signals-to-South/8211467212439/.
[41] Shim, Sun-ah. “N. Korea's Jamming of GPS Signals Poses New Threat: Defense Minister.” Yonhap News Agency (5 October 2010). http://english.yonhapnews.co.kr/national/2010/10/05/67/0301000000AEN20101005005900315F.HTML.
[42] Wesson, Kyle and Humphreys, Todd. "Unhackable Drones: The Challenges of Securely Integrating Unmanned Aircraft into the National Airspace." April 2013, draft submitted to *Scientific American*. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unhackabledrones_for_distribution.pdf: 3.
[43] Kerns et al: 3.

[44] https://www.cl.cam.ac.uk/~mgk25/ih2004-navsec.pdf: 249-250.
[45] Kerns et al: 8.
[46] Hartmann and Steup: 1.
[47] Bartles, Chuck. "Russia's Perspective on the Ways of Countering UAV Technologies." *Operational Environment Watch* (Vol. 5 Issue 4, April 2015). Foreign Military Studies Office. http://fmso.leavenworth.army.mil/OEWatch/201504/201504.pdf: 53.
[48] McLeary, Paul. "Russia's Winning the Electronic War." *Foreign Policy* (21 October 2015). http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.
[49] Concern Radio-Electronic Technologies. "Krasukha Deployed in Military Exercises." (19 October 2015). http://www.kret.com/en/news/4027/.
[50] Concern Radio-Electronic Technologies. "Eastern Military District to Receive the New Krasukha." (15 February 2015). http://www.kret.com/en/news/3656/.
[51] TASS News Agency. "Russia Developing System Capable of 'Switching Off' Foreign Military Satellites." (25 June 2015). http://tass.ru/en/russia/803788.
[52] Concern Radio-Electronic Technologies. "Krasukha Delivered Ahead of Schedule to the Russian Army." (9 October 2014). http://www.kret.com/en/news/3514/.
[53] TASS News Agency. "Foreign Buyers Interested in Russia's Krasukha Electronic Warfare Systems – Company." (26 August 2015). http://tass.ru/en/russia/816597.
[54] Heginbotham, Eric et al. "The U.S.-China Military Scorecard." (RAND Corporation, Santa Monica, CA: 2015): 249.
[55] Protek. "Automated Complex Jamming P 330M1P Diabazol." (Accessed 24 August 2016). http://www.protek-vrn.ru/production/avtomatizirovannyj-kompleks-radioelektronnogo-podavleniya-r-330m1p-diabazol/.
[56] McLeary.
[57] Perry, Bret. "How NATO Can Disrupt Russia's New Way of War." Defense One (3 March 2016). http://www.defenseone.com/ideas/2016/03/nato-russia-sof-ew-hybrid-war/126401/.
[58] Organization for Security and Co-operation in Europe. "Latest from OSCE Special Monitoring Mission to Ukraine." (10 July 2015) http://www.osce.org/ukraine-smm/171821.
[59] Schiebel Corporation. "Camcopter S-100 Unmanned Air System." (Accessed 24 August 2016). https://schiebel.net/products/camcopter-s-100-system-2/.
[60] Joint Chiefs of Staff. "Joint Operating Environment 2035." (14 July 2016): 35
[61] Ibid.
[62] Krekel: 6-7.
[63] Krekel: 80.
[64] Heginbotham et al: 281-3.
[65] LeMay Center for Doctrine. "Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations." (29 January 2015).https://doctrine.af.mil/download.jsp?filename=2-0-D06-ISR-Intel-Prep-Op-Env.pdf.
[66] United States Air Force. "RPA Vector:" 54.
[67] Northrop Grumman. "Battlefield Airborne Communications Node."
[68] Blanchard, Ben and Macfie, Nick. "U.S. Says Its Forces Will Keep Operating in South China Sea." Reuters (20 July 2016). http://www.reuters.com/article/us-southchinasea-ruling-usa-idUSKCN1000PD.

BIBLIOGRAPHY

Air Force Instruction (AFI) 90-802. *Risk Management*. Air Force Safety Center (23 March 2015). http://static.e-publishing.af.mil/production/1/af_se/publication/afi90-802/afi90-802.pdf.

Air Force Policy Directive (AFPD) 90-8. *Environment, Safety and Occupational Health Management and Risk Management.* Air Force Safety Center (2 February 2012).

Bartles, Chuck. "Russia's Perspective on the Ways of Countering UAV Technologies." *Operational Environment Watch* (Vol. 5 Issue 4, April 2015). Foreign Military Studies Office. http://fmso.leavenworth.army.mil/OEWatch/201504/201504.pdf.

Department of Defense. "Global Positioning System Standard Positioning Service Performance Standard (4th Edition)." (September 2008). http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

Dunn, Michael J. "Navstar GPS Space Segment/User Segment L5 Interfaces." Global Positioning Systems Directorate (24 September 2013). http://www.gps.gov/technical/icwg/IS-GPS-705D.pdf.

Hartmann, Kim and Steup, Christoph. "The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment." NATO Cooperative Cyber Defense Centre of Excellence Publications, 2013. https://ccdcoe.org/cycon/2013/proceedings/d3r2s2_hartmann.pdf.

Heginbotham, Eric et al. "The U.S.-China Military Scorecard." (RAND Corporation, Santa Monica, CA: 2015): 249.

Joint Chiefs of Staff. "Joint Operating Environment 2035." (14 July 2016).

Kerns, A.J., Shepard, D.P., Bhatti, J.A., and Humphreys, T.E. "Unmanned Aircraft Capture and Control via GPS Spoofing." *Journal of Field Robotics*. 31(4): 617–636, 2014. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf.

Kim, Alan et al. "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles." American Institute of Aeronautics and Astronautics (no date). https://engineering.purdue.edu/HSL/uploads/papers/cybersecurity/cyber-attack-lit-review.pdf.

Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Northrop Grumman Corporation (9 October 2009). http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

LeMay Center for Doctrine. "Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations." (29 January 2015). https://doctrine.af.mil/download.jsp?filename=2-0-D06-ISR-Intel-Prep-Op-Env.pdf.

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. "Unmanned Systems Integrated Roadmap FY2011-2036." Department of Defense (2011).

Tippenhauer, Nils Ole et al. "On the Requirements for Successful GPS Spoofing Attacks." Swiss Federal Institute of Technology, (no date). http://www.cs.ox.ac.uk/files/6489/gps.pdf.

United States Air Force. "RPA Vector: Vision and Enabling Concepts 2013–2038." Headquarters, United States Air Force (17 February 2014). http://www.af.mil/Portals/1/documents/news/USAFRPAVectorVisionandEnablingConcepts2013-2038.pdf.

Wesson, Kyle and Humphreys, Todd. "Unhackable Drones: The Challenges of Securely Integrating Unmanned Aircraft into the National Airspace." April 2013, draft submitted to *Scientific American*. http://radionavlab.ae.utexas.edu/images/stories/files/papers/unhackabledrones_for_distribution.pdf.

Yochim, Jaysen A. "The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack." U.S. Army Command and General Staff College, 6 November 2010.